

U.S. v. Gery Shalon et al.
Prepared Remarks of U.S. Attorney Preet Bharara
November 10, 2015

Good afternoon. My name is Preet Bharara, and I am the United States Attorney for the Southern District of New York.

Today, we announce criminal charges in one of the largest cyber hacking schemes ever uncovered. The charges involve cyber intrusions, over several years, targeting twelve different companies:

- seven financial institutions,
- two financial news publications,
- two software development firms,
- and a market risk intelligence company.

By any measure, the data breaches at these firms were breathtaking in scope and size:

- The defendants allegedly stole personal information for over 100 million customers, including 83 million customers from one bank alone – the largest single theft of customer data from a U.S. financial institution, ever. ***[That bank is J.P. Morgan Chas, as it has disclosed.]***
- To hide their tracks, the defendants allegedly operated their criminal schemes through over 75 shell companies; and used close to 200 identification documents fraudulently – including 30 false passports from 17 different countries.

In our view, the conduct alleged in this case showcases a brave new world of hacking for profit. It is no longer hacking merely for a quick payout.

Rather, it is hacking in support of a diversified criminal conglomerate:

- It is hacking to locate victims.
- It is hacking to spy on the competition.
- It is hacking to maximize profit.
- In short, it is hacking as a business model.

The conduct alleged in this case also, by the way, signals the next frontier in securities fraud – sophisticated hacking to steal material nonpublic information, something the defendants allegedly discussed for the next stage of their sprawling criminal enterprise.

So that's the bad news. The good news is that the FBI and the Secret Service have cracked this case, and we aim to prove it in court.

The Indictment describes the three defendants:

- Gery Shalon was the leader and self-described “founder” of this cybercriminal enterprise.
- Ziv Orenstein was his principal deputy, opening bank accounts, creating shell companies, and managing payments among cohorts.

- Joshua Aaron reported to Shalon and participated in the computer hacking and the stock manipulation scheme.

THE SCHEMES

Together, these defendants used cyber hacks into major global businesses to help advance several different criminal schemes.

First, as previously charged, Shalon, Aaron, and Orenstein ran classic pump-and-dump stock fraud schemes. They artificially inflated the price of penny stocks through false statements and manipulative trading, and then dumped their holdings before the rest of the market recognized the fraud. But for this scheme to work, the defendants needed access to a lot of names and contact information – people to whom they could pump the stock, before the defendants dumped it. They needed victims.

That is where the defendants took this classic stock fraud scheme and brought it into the cyber age. Shalon and his coconspirators hacked into the networks of seven major financial institutions and two financial news companies. Why? To get personal information for tens of millions of customers – people most likely to be engaged in significant stock trading.

They then used that stolen, private information to blast spam emails falsely touting the penny stocks that they later dumped. The valuable customer information they stole through their cyber intrusions helped generate tens of millions in stock fraud proceeds. **It was securities fraud on cyber steroids.**

Second, for many years, Shalon, Orenstein and their coconspirators also operated internet gambling businesses that generated hundreds of millions of dollars in illegal proceeds. To protect this business – like a digital don – Shalon allegedly sought to undermine rival companies by hacking and stealing their customer information and by distributing “denial of service” or DDOS cyber attacks on his rival networks. Shalon even hacked into software development firms to spy on their employees’ emails, to make sure they were not favoring his competitors.

Third, Shalon also allegedly owned and operated payment processing businesses that processed hundreds of millions of dollars in credit card payments for all types of criminal activity, including the distribution of illegal pharmaceuticals, counterfeit software, and computer malware, as well as for their own online gambling and illegal Bitcoin exchange businesses.

Shalon and his coconspirators used their cyber hacking skills to protect and advance these criminal enterprises too. For example, as alleged, Shalon cleverly hacked into a market intelligence company that worked with credit card companies to detect criminal conduct.

Shalon monitored and reviewed that company's emails so that he could stay one step ahead of their efforts to detect the very type of suspicious conduct that Shalon's payment processing businesses were engaged in.

Turbo-charged by their cyber-hacking activity, Shalon and his cohorts' criminal businesses generated hundreds of millions of dollars in illicit proceeds that Shalon concealed in bank accounts around the world.

[Go to visual]

Let me show you on this diagram how the defendants used cybercrime to help protect and advance their various criminal schemes, ranging from stock fraud to the operation of illegal gambling, payment processing and Bitcoin exchange businesses.

* * *

Shalon and Orenstein are Israeli citizens. They were arrested in Israel in July on an earlier indictment that charged them with just the securities fraud scheme, money laundering, and related crimes. We are asking Israel to extradite Shalon and Orenstein, who are both currently in custody in that country. Aaron, an American citizen, has not appeared to face the charges on the earlier indictment and remains a fugitive.

We also unsealed today an Indictment of Anthony Murgio who was previously arrested on a complaint and is charged with operating the same illegal Bitcoin exchange business as Shalon.

Partners and Thank Yous

This is not an ordinary case. To solve a case like this takes something special – it takes grit and ingenuity and collaboration of the first order. The sad truth is that, to date, complex and global cyber intrusions like these tend to go unsolved. And the criminals tend to go unprosecuted.

More often than not, the trail goes cold and the perpetrators get off. But we believe that we can change that narrative, and this case is game-changing proof. It is a testament to our partners in this groundbreaking case – the FBI and the Secret Service, who have worked together so beautifully.

This investigation started with one victim company and one hack, and as we dug deeper and used all of the investigative tools at our disposal, we were able to unearth the gargantuan scheme that you see in the charges unsealed today.

I want to thank the FBI, represented today by Assistant Director-in-Charge of the New York Field Office, Diego Rodriguez. I want to thank him, as well as Special Agent-in-Charge of the Special Operations and Cyber Branch, Ari Mahairas; Assistant Special Agent-in-Charge, Richard Jacobs; Supervisory Special Agents Jay Kramer and Lilian Perez; and Special Agents Patrick Hoffman, Joel Decapua, and Jonathan Luca.

I also want to thank the Secret Service, represented here today by Robert Sica, Special Agent-in-Charge of the New York Field Office. I want to thank him as well as Kenneth Pleasant, Assistant Special Agent-in-Charge, Supervisory Special Agent Scott Sarafian; and Special Agent Tate Jarrow.

I also must thank the dedicated career prosecutors in my office who worked so hard to make this case possible – Nicole Friedlander, Eun Young Choi, and Sarah Lai; Paul Krieger who, with Nicole, leads our Complex Frauds and Cybercrime Unit; and Ted Diskant of our Money Laundering and Asset Forfeiture Unit.

Because Shalon's cybercriminal enterprise was a global one, international cooperation was critical. We obtained evidence and legal assistance from 11 different countries. Among them, I would like to specifically recognize and thank the Israeli National Police and Ministry of Justice for their indispensable assistance.

Conclusion

Today, we have exposed a cybercriminal enterprise that for years successfully and secretly hacked into the networks of a dozen companies, stealing the personal information of over a hundred million people. The full scope and breadth of these intrusions, and the additional crimes they enabled, were revealed only after intense and coordinated law enforcement efforts.

And there are a couple of lessons here:

Even the most sophisticated companies have to appreciate the limits of their ability to understand the full scope of any cyber-intrusion and to stop the perpetrators before they strike again. If they have been hacked, most likely others have been as well and even more will be.

Their best bet to identify, stop and punish cybercriminals is to work closely – and early – with law enforcement. That happened here, and the results speak for themselves.

Speaking more broadly about the cyber threat, by now everyone appreciates that there is an army of computer saboteurs and spies and thieves and nihilists out there who wish to do us harm—who wish to upend our markets, drain our accounts, steal our secrets, halt our economic progress, and destroy our infrastructure.

But we have an army too—it comprises the best law enforcement agencies in the world; the best intelligence agencies in the world; the smartest businesspeople in the world.

Without any doubt, we have the wherewithal to withstand the cyber threat, no matter how large and how frightening.

The question is: Do we have the will? I hope this case demonstrates that we do.

* * *

Now let me call to the podium:

- Diego Rodriguez, FBI Assistant-Director-in-Charge of the NYFO.
- Robert Sica, Special Agent in Charge, U.S. Secret Service, NYFO.